

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

SEP 20 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST LOUIS

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF
2834 WYOMING STREET
ST. LOUIS, MO 63118, WITHIN THE EASTERN DISTRICT OF
MISSOURI

Case No. 4:19 MJ 7390 SPM

APPLICATION FOR A SEARCH WARRANT

I, TFO Daniel Plumb, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:
2834 WYOMING STREET, ST. LOUIS, MO 63118

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B - ITEMS TO BE SEIZED AND SEARCHED

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

21:841 AND 846

Offense Description

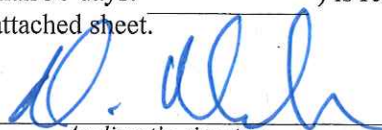
possession and conspiracy to possess with the intent to distribute controlled substance drugs

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☒ Continued on the attached sheet.

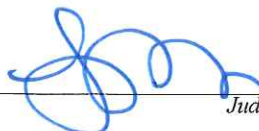
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Daniel Plumb, TFO, DEA

Printed name and title

Sworn to before me and signed in my presence.

Date: September 20, 2019City and state: St. Louis, MO*Judge's signature*

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Jillian Anderson

FILED

SEP 20 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST LOUIS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
2834 WYOMING STREET)
ST. LOUIS, MO 63118)

No.: 4:19 MJ 7390 SPM

)
) FILED UNDER SEAL
)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Daniel G. Plumb**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer with the Drug Enforcement Administration ("DEA"), and have been since January 2014. I am currently assigned to the St. Louis Division. I am a sworn police officer with over 29 years of law enforcement experience, having served with the United States Air Force, the Chesterfield Police Department and most currently the St. Peters Police Department.

2. During my tenure with DEA and as a Task Force Officer, I have been assigned to an investigative team for numerous complex investigations of drug-trafficking organizations dealing in heroin, fentanyl, cocaine, marijuana and other controlled substances. These investigations have resulted in the seizure of heroin, fentanyl, cocaine, marijuana, other controlled substances and weapons. I am familiar with and have utilized normal methods of investigation, including, but not limited to, visual surveillance, questioning of witnesses, the use of search and arrest warrants, the use of informants, the use of pen registers, the utilization of confidential sources and the use of court-authorized wire intercepts. My training with the DEA and as a sworn police officer has included specific training directly related to the aforementioned investigative techniques. I am an investigative and law enforcement officer of the United States within the

meaning of Section 2510(7) of Title 18, United States Code, and as such, I am empowered by law to conduct investigations and make arrests.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

4. Since this Affidavit is being submitted for the limited purpose of securing authorization for the acquisition of a search warrant for the **TARGET LOCATION** described herein, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish the foundation for securing authorization for establishing probable cause for the search warrant being sought.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841 (a)(1) and 846 involving the distribution and conspiracy to distribute controlled substances (hereinafter “the subject offenses”) have been committed by Antonious Lamont **BURSE** (a/k/a “B”) and/or other persons known and unknown. There is also probable cause to search the **TARGET LOCATION** described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

6. The **TARGET LOCATION** is described as a two story, multi-family residence, located at 2834 Wyoming Street, St. Louis, Missouri, 63118. The **TARGET LOCATION** is constructed of red brick and has a flat, tar paper roof, constructed of black in color material. The front porch steps are constructed of concrete. The numbers 2-8-3-4 are black in color and are displayed to the left of the front door on a white in color background. The **TARGET LOCATION** is located on the south side of Wyoming Street and faces north. The front door to the **TARGET**

LOCATION is solid with no windows and is white in color. There is a covered porch at the rear of the **TARGET LOCATION**. The back door to the **TARGET LOCATION** is solid with no windows and is white in color. The number “2” is clearly visible on the door. The remaining numbers have been removed; however, the numbers 8-3-4 are still slightly visible. The **TARGET LOCATION** is located in the City of St. Louis, within the Eastern District of Missouri. Photographs of the **TARGET LOCATION** are included in Attachment A.

TECHNICAL TERMS

7. Based on my training and experience and discussions I have had with other law enforcement officials familiar with electronic devices, I use the following technical terms to convey the following meanings:

a. “Digital device,” as used herein, includes the following terms and their respective definitions:

i) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing

devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

iii) “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

iv) A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

b. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

c. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

PROBABLE CAUSE

8. During September 2019, agents learned from a confidential source of information (“CS”) that **BURSE** was selling multigram quantities of heroin and/or fentanyl near the intersection of Nebraska and Wyoming Streets in the City of St. Louis, within the Eastern District of Missouri.¹ CS advised he/she could purchase heroin directly from **BURSE**. Agents learned that **BURSE** is currently under federal indictment in the Eastern District of Missouri, for

¹ CS – The CS has been a confidential source for a local police department for approximately one month. During this time, the CS has provided reliable information to investigators that has been independently corroborated through other investigative means. The CS has provided information that has led to the purchase and seizure of illicit drugs, heroin and fentanyl. Investigators have no reason to doubt the validity of information provided by the CS. All information provided by the CS has been and will continue to be independently corroborated by agents/officers to the fullest extent possible.

possession with intent to distribute fentanyl. A check of police databases (NCIC) confirmed **BURSE** has an active federal warrant for his arrest issued by the United States Marshal Service.

9. On September 10, 2019, your affiant met with CS. At the direction of your affiant, CS placed a recorded call to **BURSE** and arranged to meet with him to purchase \$100.00 worth of heroin. CS followed up with a text message to **BURSE** confirming the particulars of the deal/meeting location. A DEA agent, acting in an undercover capacity, transported CS to the area of Nebraska and Wyoming Streets. Once in the area, CS exited the agent's vehicle and then walked to the rear of the **TARGET LOCATION**. Moments later, **BURSE** approached CS on foot and sold CS heroin in exchange for \$100. CS later advised that **BURSE** appeared to walk from the rear of the **TARGET LOCATION**. The transaction between CS and **BURSE** was video recorded. Upon completion of the deal, CS returned to the undercover agent's vehicle and then departed the area to a neutral location. The suspected drugs sold by **BURSE** to CS field tested positive for heroin.

10. On September 12, 2019, at approximately 1:30 p.m., your affiant conducted physical surveillance of **BURSE** at the **TARGET LOCATION**. Your affiant traveled down the alley located at the rear of the **TARGET LOCATION** and observed that the back door to the **TARGET LOCATION** was standing open. From the alley, your affiant observed a male who resembled **BURSE** seated on a couch just inside the doorway at the rear of the **TARGET LOCATION**. Your affiant noticed the **TARGET LOCATION** appeared to be sparsely furnished with the only furniture visible besides the couch being a metal chair and an oscillating fan. It appeared as if **BURSE** was waiting to meet with someone. Based upon the investigation to date, agents are aware that **BURSE's** drug customers call or text message him (**BURSE**) to alert him

(**BURSE**) of their impending arrival, at which time **BURSE** exits the **TARGET LOCATION** via the back door and meets with his customers in the alley at the rear of the **TARGET LOCATION**.

11. On September 13, 2019, your affiant met with CS. At the direction of your affiant, CS sent a text message to **BURSE** and arranged to meet with him to purchase \$100.00 worth of heroin/fentanyl. A DEA agent, acting in an undercover capacity, transported CS to the area of Nebraska and Wyoming Streets. Once in the area, CS exited the agent's vehicle and then walked to the rear of the **TARGET LOCATION**. The undercover agent positioned his vehicle in a manner that allowed him to physically observe the back door and rear of the **TARGET LOCATION**. The agent noted that the door at the rear of the **TARGET LOCATION** is white in color and has a large number "2" posted near the center of the door. The agent observed **BURSE** exit the **TARGET LOCATION** via the back door marked with the number "2" and watched him approach the CS on foot. **BURSE** sold the CS heroin/fentanyl in exchange for \$100. **BURSE** then walked directly back inside the **TARGET LOCATION** via the same back door from which he originally emerged. The transaction between CS and **BURSE** was video recorded. The suspected drugs sold by **BURSE** to CS field tested positive for heroin.

12. After each controlled purchase, your affiant met with CS and confirmed that he/she did in fact purchase heroin/fentanyl directly from **BURSE**. It should be noted CS was searched for contraband prior to and after each deal with **BURSE**. Both searches confirmed CS had no contraband in his/her possession.

13. On July 3, 2019, **BURSE** was indicted by a federal grand jury in the Eastern District of Missouri with possession with the intent to distribute fentanyl, in violation of Title 21, United States Code, Section 841 Cause No. 4:19CR530 SRC SPM, for events occurring on May 11, 2019. As a result, there is an active warrant for **BURSE'S** arrest.

14. Based on your affiant's training and experience, the information set forth above is indicative of **BURSE**'s illegal possession and distribution of controlled substances at and/or from the **TARGET LOCATION**. Furthermore, based upon my training, experience and the investigation to date, investigators believe there is probable cause that evidence of the subject offenses will be found inside the **TARGET LOCATION**.

15. Additionally, based upon my and the investigating team's experience and our participation in other pending and completed narcotics and firearms investigations, I know:

- a. It is common for narcotics dealers to maintain contraband, proceeds of drug sales and records of drug transactions in their residence or other buildings under their control.
- b. Narcotic dealers maintain books, records, receipts, notes, ledgers, computer hard drives and disk records, money orders, and other papers relating to the ordering, sale and distribution of controlled substances. Narcotics dealers commonly "front" (provide drugs on consignment) crack/cocaine to their clients. The aforementioned books, records, receipts, notes, ledgers, etc. are maintained where the narcotics dealers have ready access to them, specifically in their residence or in other buildings under their control.
- c. Narcotics dealers frequently communicate with co-conspirators using digital devices, such as cellular telephones and tablets in order to arrange meetings and transactions. Further, information stored within a digital device may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, including by providing evidence of meeting locations and times, as well as the physical movements of the suspect.

- d. Narcotics dealers commonly maintain, close at hand, addresses or telephone numbers in books or papers that reflect names, addresses and/or telephone numbers for their associates in the trafficking organization.
- e. Persons involved in narcotics dealing conceal, in their residence or other buildings under their control, currency and documents reflecting ownership of vehicles and property utilized in the distribution of narcotics.
- f. Narcotics dealers take or cause to be taken photographs of themselves, their associates, their property and their product. These traffickers usually maintain these photographs in their possession and in residences and buildings under their control.
- g. Persons involved in large-scale drug-trafficking conceal in residences large amounts of currency, financial instruments, precious metals, jewelry and other items of value and/or proceeds of drug transactions, as well as evidence of financial transactions relating to obtaining, transferring, secreting or spending of large sums of money made from engaging in narcotics trafficking activities.
- h. When drug-traffickers amass large proceeds from the sale of drugs, the drug-traffickers attempt to legitimize these profits. I know that to accomplish these goals, drug-traffickers utilize, among other things, foreign and domestic banks and their attendant services, securities, cashier's checks, money drafts, letters of credit, brokerage houses, real estate, shell corporations and business fronts and records or other evidence of such is often maintained in their residence or in other buildings under their control.

- i. Records of travel related to drug trafficking activity are often maintained in the drug-trafficker's residences or in other buildings under their control, among other places.
- j. Narcotics dealers frequently keep near at hand, in their residence or other buildings under their control, paraphernalia for packaging, cutting, weighing, and distributing drugs. These paraphernalia include, but are not limited to, scales, plastic bags, and cutting agents.
- k. Evidence of occupancy and residence including, but not limited to utility and telephone bills, canceled envelopes, rental or lease agreements, and keys, is relevant evidence in narcotics and illegal firearms prosecutions.
- l. Firearms (and related ammunition and firearm parts and accessories) are a tool of narcotics traffickers, and narcotics traffickers often carry firearms or keep firearms at their residences, in other buildings under their control, in their vehicles and other locations where they sell narcotics.
- m. It is common for those possessing weapons, including those who illegally possess firearms or possess illegal firearms, to possess those firearms for long periods of time and not give up possession of the weapons unless extenuating circumstances exist.
- n. Most firearms are not manufactured within the State of Missouri and have to travel across state lines, either through sale or other means, to enter the possession of a resident of the State of Missouri.
- o. Most individuals who possess firearms tend to possess ammunition.

16. Based on my training and experience, and discussions I have had with other law enforcement officers, I am informed that individuals engaged in the criminal activities described herein typically utilize electronic devices and mobile telephones for a variety of purposes to advance and commit criminal offenses. Subjects use their device to facilitate their overall schemes and their illicit endeavors. Individuals engaged in the activities described in this affidavit use electronic devices and mobile phones for a variety of reasons including:

- a. To communicate with associates and co-conspirators before, during, and after their criminal activities, or to communicate with other non-involved third parties. They do this through via text, voice, video or photo and on applications running on the device;
- b. Accessing mapping and location services to assist in planning and facilitating their crimes, and to plan for their escape from crime scenes. Location data can indicate the user's patterns of behavior such as their physical location at the time the incidents occurred, and immediately prior to or after such incidents. It may also provide data related to the location of confederates residences, safe houses or other places used to perpetrate the crimes;
- c. Accessing contact lists of associates, confederates, and third parties;
- d. Targets take pictures and videos of themselves and associates, to memorialize their activities and fruits of their illicit activities such as contraband, firearms, and illegally obtained currency. They use the images or to brag to other confederates. These individuals frequently maintain these photographs on their electronic devices and, as described below, often post the images on social media;

- e. Criminals use the devices for online social media platforms such as Facebook, Twitter, Snapchat, etc. They communicate with their associates and confederates over such platforms. They post and display images and videos of contraband, fruits of their crimes, wealth, and otherwise memorialize criminal activities.

17. I submit that if a digital device(s) is found at the **TARGET LOCATION**, there is probable cause to believe the records described in Attachment B will be stored on that digital device(s), for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computers—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

18. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the **TARGET LOCATION** because:

- a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords.
- b. As explained herein, information stored within a computer may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my

training and experience, information stored within a computer (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or digital device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. Further, computer and digital device activity can indicate how and when the computer or digital device was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, digital device that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or digital device access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or digital device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional digital device (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information

stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for records that might be found at the **TARGET LOCATION**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other digital devices. Thus, the warrant applied for would authorize the seizure of digital device or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. In most cases, a thorough search of a premises for information that might be stored on a digital device often requires the seizure of the physical digital device and later off-site review consistent with the warrant. In lieu of removing digital device from the premises, it is sometimes possible to make an image copy of digital device. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data

recorded on the digital device, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later

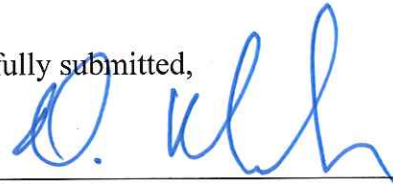
review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

19. Based upon the investigation by this affiant and other law enforcement officers, I believe **BURSE** currently utilizes the **TARGET LOCATION** to store and/or distribute controlled substances, *i.e.*, heroin and fentanyl. As a result of this investigation, there is probable cause to believe that the items listed above, which are evidence of participation in violations of Title 21, United States Code, Sections 841(a)(1) and 846 are accessible to and utilized by **BURSE** and will be found inside the **TARGET LOCATION**.

20. Due to the ongoing nature of the investigation and this affidavit, I request that this affidavit be sealed.

Respectfully submitted,



Daniel G. Plumb
Task Force Officer
Drug Enforcement Administration

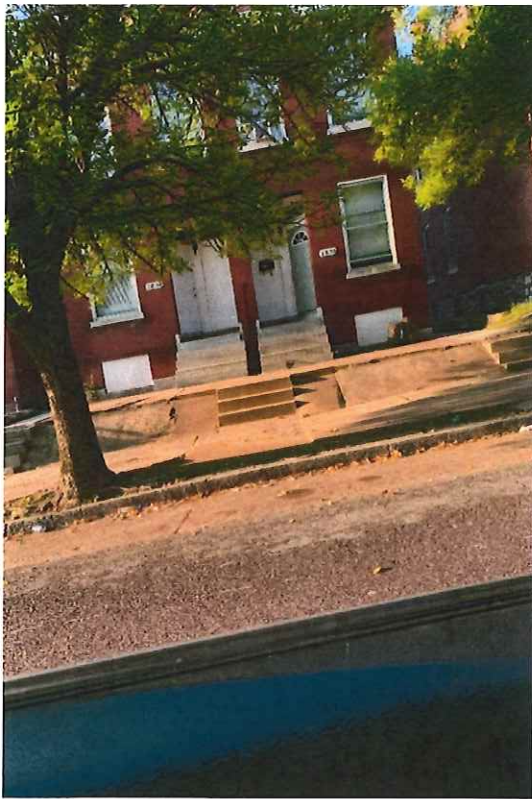
Subscribed and sworn to before me on this 20th day of September, 2019



The Honorable Shirley Mensah
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

A two story, multi-family residence, located at 2834 Wyoming Street, St. Louis, Missouri 63118. Such residence is constructed of red brick and has a flat, tar paper roof, constructed of black in color material. The front porch steps of such residence are constructed of concrete, and the numbers 2-8-3-4 are black in color and are displayed to the left of the front door on a white in color background. Such residence is located on the south side of Wyoming Street and faces north. The front door to such residence is solid with no windows and is white in color. There is a covered porch at the rear of the residence, and the back door is solid with no windows and is white in color. The number "2" is clearly visible on the back door. The remaining numbers have been removed, however the numbers 8-3-4 are still slightly visible. Such residence is located in the City of St. Louis, within the Eastern District of Missouri. Photographs of 2834 Wyoming Street, St. Louis, Missouri 63118 are set forth below (front of residence on the left and the rear of the residence on the right):



ATTACHMENT B

Property to be seized

1. All records and information relating violations of Title 21, United States Code, Sections 841 (a)(1) and 846, that constitutes fruits, evidence and instrumentalities of violations those violations involving Antonious Lamont BURSE, including:

- a. Controlled substances;
- b. Paraphernalia for packaging, cutting, weighing and distributing controlled substances, including, but not limited to, scales, baggies and spoons;
- c. Books, records, receipts, notes, ledgers, computer hard-drives and disk records, and other papers relating to the transportation, ordering, purchasing and distribution of controlled substances and/or firearms;
- d. Telephone bills, invoices, packaging, cellular batteries and/or charging devices, cancelled checks or receipts for telephone purchase/service;
- e. Cellular and/or landline telephones;
- f. Digital and/or alphanumeric text (two-way) pagers; computers capable of e-mail and/or chat-room and/or digital communication, answering machines; address and/or telephone books and papers reflecting names, addresses, and/or telephone numbers of sources of supply, of customers, and/or evidencing association with persons known to traffic in controlled substances or to facilitate such trafficking;
- g. Photographs, in particular photographs of co-conspirators, assets and/or controlled substances;
- h. United States currency, precious metals, jewelry, and financial instruments, including, but not limited to, stocks and bonds, papers, titles, deeds and other documents reflecting ownership of vehicles and property utilized in the distribution

of controlled substances or which are proceeds from the distribution of controlled substances;

- i. Books, records, receipts, pay stubs, employment records, bank statements and records, money drafts, letters of credit, money order and cashier's checks receipts, passbooks, bank checks and other items evidencing the obtaining, secreting, transfer and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money;
 - j. Papers, tickets, notes, schedules, receipts and other items relating to travel, including, but not limited to, travel to and from St. Louis, Missouri and elsewhere;
 - k. Indicia of occupancy, residency, rental and/or ownership of the vehicles and/or premises described above, including, but not limited to, utility and telephone bills, cancelled envelopes, rental or lease agreements and keys; and
 - l. Firearms and/or weapons.
2. Computers and mobile cellular phones (hereinafter "Device(s)") used as a means to commit the violations described above.